Kim D. Stephens
kstephens@tousley.com
Christopher I. Brain
cbrain@tousley.com
Jason T. Dennett
jdennett@tousley.com
Tousley Brain Stephens PLLC
1700 Seventh Avenue, Suite 2200
Seattle, WA 98101
Tel: (206) 682-5600
Fax: (206) 682-2992

Interim Lead Plaintiffs' Counsel

Keith S. Dubanevich
kdubanevich@stollberne.com
Yoona Park
ypark@stollberne.com
Stoll Berne Lokting
& Shlachter P.C.
209 SW Oak Street, Suite 500
Portland, OR 97204
Tel: (503) 227-1600
Fax: (503) 227-6840

Interim Liaison Plaintiffs' Counsel

[*Additional counsel appear on the signature page.*]

IN THE UNITED STATES DISTRICT COURT

FOR THE DISTRICT OF OREGON

IN RE: PREMERA BLUE CROSS CUSTOMER DATA SECURITY BREACH LITIGATION This Document Relates to All Actions	Case No. 3:15-md-2633-SI **PLAINTIFFS' REPLY IN SUPPORT OF MOTION FOR SANCTIONS FOR DEFENDANT'S DISCOVERY MISCONDUCT** **FILED UNDER SEAL**

TABLE OF CONTENTS

Page

Premera destroyed critical trial evidence in the midst of this litigation before Plaintiffs could examine it. The jury should be so informed, and Premera should be barred from making any argument that could have been disproved by the evidence it destroyed.

Plaintiffs contend that Premera did not provide the data security it was obligated to provide. Premera has defended itself from these allegations primarily by maintaining that—while hackers roamed freely in its computer systems for the better part of a year—hackers did not actually "bulk remove" any of the information that they accessed. Setting aside that this argument is an improper attempt to distract the jury from the actual claims in this case, *Premera destroyed the evidence that would have disproven its assertion.* In particular, Premera destroyed a computer (designated "A23567-D") and critical logging information ("DLP logs") that would have shown whether hackers removed class members' data. It is fundamentally unfair to allow Premera to make such arguments when it destroyed the evidence that would disprove them.

Premera's core argument in opposition is that Plaintiffs failed to cite Rule 37(e) in their initial motion. While Premera is right about the governing rule, it is wrong about the result, and Plaintiffs ask this Court to hold that: (1) Plaintiffs are entitled to an adverse jury instruction at trial stating that given the spoliation, the jury is to presume that exfiltration occurred; (2) no expert or fact witness can opine that there was no evidence of data exfiltration, based on the Mandiant report or otherwise; and (3) Premera may not introduce any evidence that relates to the computer or logs that it destroyed.

I. RULE 37(E) GOVERNS THIS MOTION.

Premera is correct that Rule 37(e) governs this motion, and Plaintiffs apologize for their failure to cite this rule initially. Under Rule 37(e), the Court may, upon finding prejudice, order sanctions necessary to cure such prejudice when electronically stored information that (1) should have been preserved (2) has been lost, (3) because a party failed to take reasonable steps to

preserve it, (4) and it cannot be restored or replaced through additional discovery. Plaintiffs must show intent to receive an adverse inference instruction, although *not* for any other requested form of relief. *See* Rule 37(e) Committee Notes on Rules – 2015 Amendment.

II. PREMERA WRONGFULLY DESTROYED A COMPUTER THAT CONTAINED CRITICAL, UNIQUE EVIDENCE.

A. Premera should have preserved the computer, but failed to do so.

As explained in Plaintiffs' opening brief, Premera destroyed a computer (A23567-D) that contained critical evidence. Premera's own expert specifically instructed Premera to preserve this computer, Sherer Decl. Ex. 2, and Premera does not deny that it failed to do so. Plaintiffs have thus established the first two elements required for sanctions under Rule 37(e).

B. Premera failed to take reasonable steps to preserve the computer.

Premera half-heartedly argues that it took appropriate steps to preserve the computer. It offers no evidence in support of that contention, which is insufficient. *See Blumenthal Distrib., Inc. v. Herman Miller, Inc.*, 2016 WL 6609208, at 17 (C.D. Cal. 2016) (ordering adverse inference where party offered only vague information about allegedly inadvertent deletion), *adopted* 2016 WL 6901696 (C.D. Cal. 2016). Instead, Premera offers vague, unsubstantiated and unreasonable explanations largely in the passive voice about "[i]nadvertent errors" by unknown individuals, "accidentally recycling" by inchoate forces, and "los[ing] track of" crucial evidence for unspecified reasons. Premera thus does not and cannot show it took "reasonable steps." *See id*.

C. The computer cannot be replaced or restored by other discovery.

Premera's final argument against sanctions is that other discovery will suffice. Not so.

1. Any FBI analysis would be unlikely to substitute the computer itself.

Premera's first argument is that FBI analysis can substitute for the missing computer. In

particular, Premera claims, without evidentiary support, that the FBI did not capture a forensic image of the computer and thus the Court should conclude that the computer did not contain important information. Dkt. 203 at 7. This is incorrect. First, if true, this assertion shows only that Premera does not believe the FBI imaged a particular computer, not what the FBI actually did. Second, even if the FBI did not image the computer, this says nothing about *why* the FBI did not image that particular computer at that particular time, much less substitute for Plaintiffs' own examination. This indicates nothing about the FBI's investigation, methods, goals, or conclusions. Third, the FBI apparently will *not* share what information they do have with Plaintiffs, nor has Premera produced any FBI report. [1] *See* Supplemental Declaration of Jason T. Dennett (2nd Dennett Decl.) at ¶ 2.

2. Premera cannot offer its own expert's conclusions in place of the computer.

Premera next argues that its own hired expert report should substitute for the computer. Unsurprisingly, the law is to the contrary. *PacificCorp v. Nw. Pipeline GP*, 879 F. Supp. 2d 1171, 1190. (D. Or. 2012) ("[F]orcing a party to rely on evidence selected by an opposing party's expert creates prejudice, because such evidence generally supports that party's case."). This general rule is particularly relevant here because Premera's expert (Mandiant) has changed its story in this litigation regarding other critical evidence, which demonstrates that it is willing to change its conclusions for the benefit of its client. Dennett Decl. Ex. 1, 3-4.[2]

3. Crowdstrike's examination does not replace or restore the computer.

Premera next argues that the so-called "Crowdstrike" examination substitutes for the

[1] Premera did not produce—or note on a privilege log—any FBI report. Indeed, Premera's 30(b)(6) witness confirmed that he did not know what the FBI did. 2nd Dennett Decl. Ex. 10.

[2] Mandiant initially concluded that the deleted RAR files were more than likely created by the attacker, but watered down its conclusions after Premera had an opportunity to edit the report.

computer. It does not. *That company specifically disclaimed any investigation about the very issue now before the Court,* stating specifically that it was *not* able to "identify intrusion related activity outlined in the Mandiant report." Sherer Decl. Ex. 7 at PBC00169146. Compounding this issue, Premera appears to have wiped the computer in 2015; i.e., Crowdstrike likely examined the computer *after* Premera destroyed the evidence.

D. The Court should find that Premera intentionally destroyed the computer.

Premera had a standard policy of wiping and reformatting the hard drives of computers infected with malware; i.e., a policy of destroying evidence. Indeed, just a few months before Premera discovered this breach, the senior manager for information security explained to his employees that the "correct set of procedures" for any malware infection was to wipe its hard drive—with no backup—and then restore the computer to its original settings before returning it to service. *See* 2nd Dennett Decl. Ex. 1; *cf. also id*. ("I have directed the team to ***wipe* these machines and virtual images (WITH NO BACKUP)**." (emphasis in original) (referring to a different malware infection)). This was so even though employees pointed out that Premera should *not* destroy computers in this manner because it needed to "preserve forensic evidence" for "future review." 2nd Dennett Decl. Ex. 3.

Premera apparently concedes that its standard policy is to destroy evidence intentionally, *see id*., because Premera claims that it absolutely did *not* follow its standard policy with respect to A23567-D and instead "unintentionally" filed this computer as "End of Life" equipment and so stored it offsite, "offline and unused." Dennett Decl. Ex. 7 (quoting Premera Interrogatory Response #14). This unsupported claim is contradicted by the evidence: computer A23567-D was returned to service and on its network in 2016. *Compare* Sherer Decl. Ex. 7 at PBC00169146 (stating that Crowdstrike examined "*the Premera network*" in April 2016); *with id.* at PBC00169161 (stating that Crowdstrike examined computer A23567-D).

The above is more than sufficient to show that Premera intentionally destroyed computer A23567-D's hard drive pursuant to its standard policy. This is particularly so given that a Premera employee *specifically* alerted the company to the fact that its standard policy was to improperly destroy important "forensic evidence." 2nd Dennett Decl. Ex. 3. Plaintiffs ask the Court not to accept Premera's vague explanation (contradicted by the evidence) that it only destroyed A23567-D accidentally. *See First Fin. Sec., Inc. v. Freedom Equity Grp., LLC*, 2016 WL 5870218, at 3 (N.D. Cal. 2016) (ordering adverse instruction and rejecting argument that deletion was inadvertent because of a routine habit of deleting particular data).

E. Premera prejudiced Plaintiffs by destroying the computer.

One of Premera's defenses in this litigation is to attempt to prove that the hackers did not bulk remove Plaintiffs' personal information. To make this unlikely claim, Premera's testifying experts rely entirely on the report that Premera hired *another* expert firm—Mandiant—to produce. *See* Dkt. 192 at 6, 12-14 (Campbell Declaration); Dkt. 191 at 16-17 (Anderson). And *that* report claims that the very computer that Premera destroyed *proves* that hackers did not bulk exfiltrate Plaintiffs' data. In particular, and as discussed in Plaintiffs opening motion on pages 5 and 6, *A23567-D is the only computer on Premera's network that hosted a type of malware called PHOTO*, the malware that would have been used for any exfiltration. *See* Strebe Decl. ¶ 229.

It would severely prejudice Plaintiffs if the Court allowed Premera to argue that no data was exfiltrated after Premera destroyed the only evidence that could refute that argument. Plaintiffs' request relief sufficient to prevent this prejudice. *Accord Matthew Enter., Inc. v. Chrysler Grp. LLC*, 2016 WL 2957133, at 3 (N.D. Cal. 2016) ("Rule 37(e) intentionally leaves to the court's discretion exactly what measures are necessary.").

* * *

One final point. Premera's characterization of Plaintiffs' discovery efforts is false. Plaintiffs sought to conduct their own forensic analysis of Premera's entire network. Dennett Decl. Exhibit 2. Premera suggested review of the "affected systems as identified by Mandiant" as a compromise, which Plaintiffs accepted. 2nd Dennett Decl. Ex. 5.

III. PREMERA SHOULD BE SANCTIONED FOR DESTROYING ITS DATA LOSS PREVENTION LOGS, WHICH IT DID NOT ATTEMPT TO PRESERVE.

A. DLP logs were critical, and Premera did not attempt to preserve them.

At issue in this portion of Plaintiffs' motion are Premera's Data Loss Prevention ("DLP") logs. The DLP system logged any attempt to email PII or PHI outside Premera's network. 2nd Dennett Decl Ex. 6 and 7; Ex. 8; Christian Decl. at ¶ 15. There is no substitute for the DLP logs, and Premera does not convincingly contend otherwise.[3] In particular, Plaintiffs need DLP logs because the attackers could have exfiltrated data by emailing files out of Premera's network, which Premera DLP logs would have recorded.

Premera offers no explanation for its failure to even *attempt* to preserve the DLP logs, nor does it meaningfully contest that the DLP logs contained evidence relevant to this litigation or that Premera destroyed that evidence.

B. So-called "Vontu" emails do not replace or restore what Premera destroyed.

A DLP system has a number of loss prevention functions, one of which is to produce what are called "Vontu alert emails." Premera contends that these e-mails substitute for the logs themselves, but this is not so in two respects. First, Premera apparently only produced *three* unique Vontu alert e-mails. *See* Declaration of Cecily Shiel. Even if the complete set of such e-mails could replicate the logs, Premera apparently is unable to produce them. In any event,

[3] Premera's reference to "RAR files" (compressed files that hackers *could* have used to exfiltrate data) is far off-point because such files have little to do with the DLP logs, which logs would have shown whether hackers simply e-mailed Plaintiffs' information out of Premera's network.

Premera has never actually contended that Vontu e-mails would contain all of the same information about exfiltration as the logs that Premera destroyed.

Plaintiffs note that the "logs" that Plaintiffs' expert Mr. Strebe discussed in the deposition excerpt Premera cites were *Windows* logs, not DLP logs. Sherer Decl. Ex. 5, Strebe Dep. At 242:22-243:55. It is misleading for Premera to contend that one has any relationship to the other.

C. Premera seriously prejudiced Plaintiffs by destroying the DLP logs, and it was not reasonable to destroy them.

When Premera destroyed the DLP logs, Premera destroyed the only complete set of evidence that would show whether the attackers used email to exfiltrate PII. Such logs should have been preserved at the time Premera issued its first litigation hold. *Blumenthal*, 2016 WL 6609208 at 16 (loss of evidence not reasonable where party "never instituted a proper litigation hold."). The fact that Premera claims the logs were actually destroyed during Premera's transition between electronic systems is no excuse. *See Matthew Enter.*, 2016 WL 2957133, at 1 (loss of evidence not reasonable under Rule 37(e) where party "discarded all its old messages while switching email providers."). Premera's failure to even attempt to preserve these logs was not reasonable, and it should not be able to benefit by destroying them. *See id*.

Dated: October 23, 2018

Respectfully Submitted,

TOUSLEY BRAIN STEPHENS PLLC

By: *s/ Kim D. Stephens*
Kim D. Stephens, P.S., OSB No. 030635
Christopher I. Brain, *admitted pro hac vice*
Jason T. Dennett, *admitted pro hac vice*
1700 Seventh Avenue, Suite 2200
Seattle, WA 98101
Tel: (206) 682-5600
Fax: (206) 682-2992
Email: kstephens@tousley.com
cbrain@tousley.com
jdennett@tousley.com

Interim Lead Plaintiffs' Counsel

STOLL BERNE

By: *s/ Keith S. Dubanevich*
Keith S. Dubanevich, OSB No. 975200
Yoona Park, OSB No. 077095
209 SW Oak Street, Suite 500
Portland, OR 97204
Tel: (503) 227-1600
Fax: (503) 227-6840
Email: kdubanevich@stollberne.com
ypark@stollberne.com

Interim Liaison Plaintiffs' Counsel

Tina Wolfson
AHDOOT & WOLFSON, PC
10728 Lindbrook Drive
Los Angeles, CA 90024
Tel: (310) 474.9111
Fax: (310) 474.8585
Email: twolfson@ahdootwolfson.com

James Pizzirusso
HAUSFELD LLP
1700 K. Street NW, Suite 650
Washington, DC 20006
Tel: (202) 540.7200
Fax: (202) 540.7201
Email: jpizzirusso@hausfeld.com

Karen H. Riebel
LOCKRIDGE GRINDAL NAUEN P.L.L.P.
100 Washington Ave. South, Suite 2200
Minneapolis, MN 55401
Tel: (612) 596-4097
Email: khriebel@locklaw.com

Plaintiffs' Executive Leadership Committee

6010/001/523443.1